AN A.S. PRATT PUBLICATION
SEPTEMBER 2025
VOL. 11 NO. 7

# PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

**EDITOR'S NOTE: IT'S ABOUT DATA** Victoria Prussen Spears

**DATA PRIVACY IMPLICATIONS OF DOJ BULK SENSITIVE PERSONAL DATA RULE UNDER EXECUTIVE ORDER 14117 AS SEEN THROUGH THE LENS OF VENDOR CONTRACTING AND INTERNATIONAL NORMS**
Frederick C. Bingham, Jeewon K. Serrato and Shruti Bhutani Arora

**STEERING CLEAR OF ECPA LIABILITY: WHAT CONNECTED VEHICLE COMPANIES SHOULD KNOW ABOUT RESPONDING TO GOVERNMENT PROCESS**
Ian L. Barlow, Brandon J. Moss and Elizabeth K. Drill

**HOW SAFE IS YOUR MULTI-FACTOR AUTHENTICATION? COMPLYING WITH THE NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES AND OTHER CYBERSECURITY REGULATORS**
Mark L. Krotoski, Brian H. Montgomery and Johnna Purcell

**NINTH CIRCUIT PRIVACY RULING COULD BE USED TO EXPAND POTENTIAL FORUMS FOR E-COMMERCE LAWSUITS**
Attison L. Barnes, III, Duane C. Pozza, Enbar Toledano and Leah C. Deskins

**CALIFORNIA PRIVACY PROTECTION AGENCY INTENSIFIES ENFORCEMENT: RECENT ENFORCEMENT ACTIONS AND TRENDS**
Arsen Kourinian, Lei Shen, Amber C. Thomson and Megan P. Von Borstel

# Pratt's Privacy & Cybersecurity Law Report

VOLUME 11 NUMBER 7 September 2025

**Editor's Note: It's About Data** 205
Victoria Prussen Spears

**Data Privacy Implications of DOJ Bulk Sensitive Personal Data Rule Under Executive Order 14117 as Seen Through the Lens of Vendor Contracting and International Norms** 207
Frederick C. Bingham, Jeewon K. Serrato and Shruti Bhutani Arora

**Steering Clear of ECPA Liability: What Connected Vehicle Companies Should Know About Responding to Government Process** 218
Ian L. Barlow, Brandon J. Moss and Elizabeth K. Drill

**How Safe Is Your Multi-Factor Authentication? Complying With the New York State Department of Financial Services and Other Cybersecurity Regulators** 223
Mark L. Krotoski, Brian H. Montgomery and Johnna Purcell

**Ninth Circuit Privacy Ruling Could Be Used to Expand Potential Forums for E-Commerce Lawsuits** 229
Attison L. Barnes, III, Duane C. Pozza, Enbar Toledano and Leah C. Deskins

**California Privacy Protection Agency Intensifies Enforcement: Recent Enforcement Actions and Trends** 232
Arsen Kourinian, Lei Shen, Amber C. Thomson and Megan P. Von Borstel

LexisNexis®

## QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:

| | |
|---|---|
| Deneil C. Targowski at | (908) 673-3380 |
| Email: | Deneil.C.Targowski@lexisnexis.com |

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

| | |
|---|---|
| Customer Services Department at | (800) 833-9844 |
| Outside the United States and Canada, please call | (518) 487-3385 |
| Fax Number | (800) 828-8341 |
| LexisNexis® Support Center | https://supportcenter.lexisnexis.com/app/home |

For information on other Matthew Bender publications, please call

| | |
|---|---|
| Your account manager or | (800) 223-1940 |
| Outside the United States and Canada, please call | (518) 487-3385 |

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

*An A.S. Pratt Publication*
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2025–Pub. 4939)

# *Editor-in-Chief, Editor & Board of Editors*

*Pratt's Privacy & Cybersecurity Law Report* is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. Copyright 2025 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

# How Safe Is Your Multi-Factor Authentication? Complying With the New York State Department of Financial Services and Other Cybersecurity Regulators

*By Mark L. Krotoski, Brian H. Montgomery and Johnna Purcell**

*Vulnerabilities in multi-factor authentication (MFA) can be exploited to gain access to systems resulting in costly enforcement actions for those companies that fall victim to those attacks. The authors of this article discuss MFA regulatory compliance and advise companies to take steps to ensure that MFA protections are in place as part of a cybersecurity ecosystem and that the type of MFA that is used is resistant to common attack vectors such as social engineering and phishing.*

The use of Multi-Factor Authentication (MFA) is a cybersecurity best practice which ensures the security and reliability of systems and networks integral to government operations, critical infrastructure, and corporate functions. Cybersecurity experts in both the public and private sectors recognize that MFA is an integral part of a sophisticated cybersecurity enterprise. In fact, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has found that the "use of MFA on your accounts makes it 99% less likely" that the user will be hacked,[1] and recommend that entities of all sizes adopt MFA as part of their layered cybersecurity approach.[2] Some state and federal regulatory agencies such as the New York Department of Financial Services (NYDFS) and Federal Trade Commission (FTC) require that covered entities have MFA or similar cybersecurity protections in place in order to protect consumer's sensitive data.

However, as CISA has observed, "not all forms of MFA are equally secure."[3] Vulnerabilities in MFA can be exploited by threat actors to gain access to systems resulting in costly enforcement actions for those companies that fall victim to those

* Mark L. Krotoski is a litigation partner and cyber disputes leader at Pillsbury Winthrop Shaw Pittman LLP. Brian Montgomery is a regulatory partner and consumer finance leader at the firm. Johnna Purcell, an associate at the firm, focuses on matters related to cyber policy, financial services and national security. The authors may be reached at mark.krotoski@pillsburylaw.com, brian.montgomery@pillsburylaw.com and johnna.purcell@pillsburylaw.com, respectively.

[1] CISA, Multifactor Authentication, https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication.

[2] See id.; see also NIST, Multi-Factor Authentication, https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication.

[3] CISA, Implementing Phishing-Resistant MFA, https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf.

attacks. All companies should take proactive steps to ensure that MFA protections are in place as part of a layered, zero-trust cybersecurity ecosystem and that the type of MFA that is used is resistant to common attack vectors such as social engineering and phishing.

## MFA AND ITS VULNERABILITIES

MFA operates as a digital authentication tool by requiring more than one distinct authentication factor for successful authentication. Three common authentication factors include:

1. *Something You Know*: A password or the answer to a security question.
2. *Something You Have*: A code that was sent via SMS to a cell phone, an authentication application installed to a cell phone, or an identification card or badge.
3. *Something You Are*: Biometrics such as a fingerprint, facial recognition scan, or vocal pattern.

At its most basic level, MFA operates as another tool for identity management and verification which provides an additional layer of security on top of traditional username and password protections.

There are many types of MFA. Most common is MFA based on a push notification or text message verification which requires the user to approve device and network sign ins on a second device. Other MFA types include:

- *Virtual MFA Devices*: Uses an application to generate an authentication code that must be provided before access is granted.
- *U2F Security Key*: Uses a physical U2F key to authenticate the user's identity. The U2F key is plugged into the computer and once a password is entered the network will ping the U2F key with a cryptographic challenge which the user responds to by taping the U2F key.
- *Hardware MFA Device*: Uses a hardware token as a physical security key that is typically plugged into or tapped into a device to verify the user's identity before permitting access.
- *SMS Text Message-Based MFA*: Uses a one-time passcode sent to the user via text message that must be provided before access is granted.

Given that cyber adversaries are increasingly capable of guessing or harvesting passwords to gain illicit access to networks – MFA exponentially enhances security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and, as such, will be denied access to the targeted network.

However, like any cybersecurity layer, MFA is not without its own unique vulnerabilities. MFA is particularly vulnerable to phishing attacks. Phishing is a common form of cyberattack in which a hacker will attempt to trick an individual into revealing sensitive information, such as usernames and passwords, by pretending to be a trustworthy entity. In the MFA setting, phishing can be used to bypass identity management mechanisms by misleading users into revealing the unique code or passkey that was provided to them to verify their identity. For example, one common technique that attackers will use is generating an email link asking for a user to verify their account details. The link in that email will take the user to a fake website that the hacker has created which mirrors the legitimate login site. The counterfeit site will prompt users to enter their login credentials and MFA code or pin. The hacker will monitor the website and, once it obtains the user's credentials, use it to access the protected account or network.

Fortunately, there are forms of MFA that are resistant to phishing attacks. Phishing-resistant MFA refers to authentication methods that are specifically designed to prevent attackers from bypassing the MFA process, even if they manage to trick users into revealing their login credentials. This includes U2F security keys, hardware MFA devices, and biometric MFA verification, all of which are more difficult to intercept than code-based MFA methods. CISA has instructed that "phishing-resistant MFA is the gold standard, and organizations should make migrating to it a high priority effort."[4]

Additionally, MFA should be considered along with other measures as part of a layered cybersecurity ecosystem designed to detect, deter, and remediate cyber incidents.

## REGULATORY MFA RECOMMENDATIONS AND REQUIREMENTS

Recognizing the value that MFA offers to corporations, consumers, and even governmental agencies, regulators at the state and federal levels have adopted policies that recommend or, in some cases, require the use of MFA.

As one prominent example, the NYDFS's Cybersecurity Regulation explicitly requires covered entities to implement MFA. Specifically, the regulation mandates that organizations use MFA to secure access to sensitive systems, data, and applications for both employees and third-party service providers accessing the company's internal networks from an external network. In place of MFA, a covered entity's chief information security officer may approve, in writing, the use of reasonably equivalent or more secure access controls.[5] The guidance provides this flexibility so that organizations can adopt innovative security technologies that might prove even more effective than MFA, following internal review and approval.

Additionally, beginning on November 1, 2025, the scope of the MFA requirement under the NYDFS Cybersecurity Regulation will expand. By that date, covered entities must ensure that MFA is implemented for all individuals accessing any covered entity's

[4] Id.

[5] 23 NYCRR § 500.12

information systems, regardless of location, user type, or the nature of the data involved. Exceptions will be permitted only when a covered entity's CISO has formally approved, in writing, the use of reasonably equivalent or stronger compensating controls which are subject to periodic, and at minimum annual, review or where the covered entity qualifies for a limited exemption.[6] The limited exceptions contemplated under the regulation apply to covered entities that meet any of the following thresholds: fewer than 20 employees and independent contractors, including those of affiliates, less than $7.5 million in gross annual revenue in each of the last three fiscal years from the covered entity and its affiliates' New York operations, or less than $15 million in year-end total assets, inclusive of affiliates, as calculated under generally accepted accounting principles. If a covered entity qualifies for an exception, then MFA will only be required for remote access to the covered entity's information systems, remote access to third-party applications, including but not limited to cloud-based platforms, from which nonpublic information can be accessed, and all privileged accounts other than service accounts that do not permit interactive login.

The regulation and associated guidance encourage the use of strong MFA methods, such as hardware tokens, biometrics, or other advanced methods that are resistant to common cyber threats like phishing. NYDFS has observed since its cyber regulation went into effect in 2017 that MFA is a common vulnerability that is exploited in attacks on entities that are subject to the regulation's requirements.[7] These cyberattacks have palpable consequences for the companies that experience them and their customers. In a single year more than 18.3 million consumers were impacted by cyber incidents that were reported to NYDFS.[8] As a result, NYDFS decided to strengthen the MFA mandate in its cybersecurity regulation through a 2023 amendment to the regulation. What's more, in June 2025, NYDFS issued an industry letter in response to ongoing global conflicts, emphasizing that escalating geopolitical instability significantly increases cyber risk across the financial sector. The Department urged regulated entities to reassess their cybersecurity programs with a heightened focus on core controls including multi-factor authentication.[9]

NYDFS is not the only regulatory body which recognizes the benefits for consumers of implementing MFA. For example, a 2014 Executive Order on Improving the Security of Consumer Financial Transactions highlighted the importance of adopting stronger

[6] NYDFS, Cybersecurity Resource Center: FAQs (last accessed: Jul. 24, 2025), https://www.dfs.ny.gov/industry_guidance/cybersecurity.

[7] NYDFS Industry Letter to All Regulated Entities Regarding Guidance on Multi-Factor Authentication (Dec. 7, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211207_mfa_guidance.

[8] Id.

[9] Executive Order No. 13681 – Improving the Security of Consumer Financial Transactions (Oct. 17, 2014), https://www.govinfo.gov/content/pkg/DCPD-201400778/pdf/DCPD-201400778.pdf.

security measures, including the implementation of MFA to protect consumers' financial information.

Specifically, it encouraged the financial sector to move toward more secure authentication practices, such as multi-factor authentication, to reduce fraud and enhance the security of consumer transactions. The executive order recognized that using multi-factor authentication could significantly strengthen the protection of sensitive financial data by making it harder for unauthorized individuals to gain access to accounts, even if login credentials are compromised.

In addition, the FTC also adopted amendments to its Safeguards Rule that incorporated significant portions of the NYDFS cybersecurity regulation, including the requirement to implement MFA or reasonably equivalent or more secure access controls.[10]

## MFA ENFORCEMENT ACTIONS

Many corporations have faced state and federal enforcement actions based, in part, on their failure to implement MFA. These enforcement actions typically fall into two categories: (1) enforcement actions stemming from failure to implement MFA where specifically required by regulation, and (2) enforcement actions arising from liability associated with a cyberattack or security breach where the failure to implement MFA is evidence of deficient cybersecurity protections. In both cases, the failure to have in place effective MFA has proven costly for corporations.

### Failure to Implement MFA When Required

At the beginning of the year, the NYDFS reached a settlement with a financial services provider that did not require customers to utilize MFA on their accounts. During its investigation of a December 2022 data breach that left customer social security numbers vulnerable to exposure and exploitation, NYDFS found that the financial services provider did not require customers to use MFA to access their accounts.[11] This constituted a violation of the provider's own policy as well as the NYDFS cybersecurity regulation. The financial services provider subsequently remediated this security vulnerability and now requires customers to utilize MFA protections. In the enforcement action, the financial services provider was also fined $2 million dollars by NYDFS.

### Security Breach Exploiting the Absence of MFA

While not all regulatory frameworks mandate MFA, the absence of MFA has served as a key finding in enforcement actions. For example, the Securities and Exchange

[10] FTC, FTC Amends Safeguards Rule to Require Non-Banking Financial Institutions to Report Data Security Breaches (October 27, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-amends-safeguards-rule-require-non-banking-financial-institutions-report-data-security-breaches.

[11] NYDFS, Superintendent Adrienne A. Harris Secures $2 Million Cybersecurity Settlement with PayPal, Inc. (Jan. 23, 2025), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20250123.

[12] 17 C.F.R. § 248.30(a).

Commission (SEC) promulgated its version of the Safeguards Rule, which requires broker-dealer and investment advisors that are registered with the SEC to adopt written policies and procedures to protect customer data from unauthorized access.[12] While the SEC's Safeguards Rule does not explicitly mandate MFA, the absence of these protections has been a focal point of enforcement actions following a data breach. In two recent enforcement actions, the SEC specifically pointed to the covered entities' failure to utilize MFA as a factor which notably contributed to the exposure of customer information. In both cases, the companies ultimately were required to pay the SEC more than $250,000 to settle their respective enforcement actions.[13]

## RECOMMENDATIONS FOR REGULATORS AND COMPANIES

As government agencies have noted, not all MFA is equally secure. Organizations that have in place MFA that is vulnerable to exploitation could still face cyberattacks that lead to costly investigations, litigation, and enforcement actions. Thus, while basic forms of MFA *might* currently fulfill regulatory requirements or serve as successful defenses to enforcement actions – it is unlikely that those protections alone will suffice in deterring cyberattacks in the long term.

MFA provides important access controls to limit network or account access to appropriate users. As part of an organization's cyber risk assessment, they should first review whether MFA is in place and second whether a more secure form of phishing-resistant MFA might be appropriate considering the specific risks to their business operations and customers. Waiting until a regulatory requirement is in place or litigation is already underway is costly both due to the severe penalties associated with enforcement actions and the reputational harm that comes from a breach of customer or other sensitive data.

[13] See In the Matter of Cambridge Investment Research, Inc. and Cambridge Investment Research Advisors Inc., File No. 3-20496; In the Matter of Cetera Advisor Networks LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, Cetera Advisors LLC, and Cetera Investment Advisers LLC, File No. 3-20490.